From: Ritchey, Gail (COT)
Sent: Wednesday, August 15, 2007 9:54 AM
To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members
Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group
Subject: COT Security Alert - Microsoft Security Bulletins for August

COT Security Alert

Microsoft has just released the Microsoft Security Bulletins for August. There are **six critical** bulletins, **three important** bulletins for August. Various vulnerabilities are addressed in the bulletins. Details of the vulnerabilities and their impact are provided in the links listed.

MS07-042 Critical: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)
http://www.microsoft.com/technet/security/bulletin/ms07-042.mspx

MS07-043 Critical: Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)
http://www.microsoft.com/technet/security/bulletin/ms07-043.mspx

MS07-044 Critical: Vulnerability in Microsoft Excel Could Allow Remote Code Execution (940965)
http://www.microsoft.com/technet/security/bulletin/ms07-044.mspx

MS07-045 Critical: Cumulative Security Update for Internet Explorer (937143)
http://www.microsoft.com/technet/security/bulletin/ms07-045.mspx

MS07-046 Critical: Vulnerability in GDI Could Allow Remote Code Execution (938829)
http://www.microsoft.com/technet/security/bulletin/ms07-046.mspx

MS07-047 Important: Vulnerability in Windows Media Player Could Allow Remote Code Execution (936782)
http://www.microsoft.com/technet/security/bulletin/ms07-047.mspx

MS07-048 Important: Vulnerabilities in Windows Gadgets Could Allow Remote Code Execution (938123)
http://www.microsoft.com/technet/security/bulletin/ms07-048.mspx

MS07-049 Important: Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (937986) http://www.microsoft.com/technet/security/bulletin/ms07-049.mspx

MS07-050 Critical: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)
http://www.microsoft.com/technet/security/bulletin/ms07-050.mspx

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Confidentiality Statement - This communication contains information which is confidential. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any form of distribution, copying, forwarding or use of this communication or the information therein is strictly prohibited and may be unlawful. If you have received this communication in error, please return it to the sender and send a copy or notify: securitynotice@ky.gov and then delete the communication and destroy any copies.

Security Administration Branch
Division of Technical Services
Commonwealth Office of Technology
101 Cold Harbor Drive
Frankfort, KY 40601
Commonwealth Service Desk Phone: 502.564.7576
CommonwealthServiceDesk@ky.gov
COTSecurityServicesISS@ky.gov